FORESCOUT

OT:ICEFALL Vulnerability Research Disclosure

Updated – November 29, 2022

Q: What is OT:ICEFALL?

A: Vedere Labs disclosed on June 21, 2022 a set of 56 new vulnerabilities we are collectively calling "OT:ICEFALL". These vulnerabilities affect devices from 10 major OT manufacturers. The vulnerabilities in OT:ICEFALL are divided into four main categories:

- Insecure engineering protocols
- Weak cryptography or broken authentication schemes
- Insecure firmware updates
- Remote code execution via native functionality

It has been 10 years since Project Basecamp, a research project conducted by Digital Bond that investigated how critical operational technology (OT) devices and protocols were, to use the term they coined: "insecure by design." Since then, we have seen hugely impactful real-world OT malware, such as Industroyer, TRITON, Industroyer2 and INCONTROLLER, abusing insecure-by-design functionality. In the past decade, the amount of OT vulnerability disclosures has been going up steadily as the community has focused on this problem, but we still have a mountain to climb with these devices and protocols.

On November 29, we disclosed three more vulnerabilities continuing the OT:ICEFALL work. These new vulnerabilities affect Festo automation controllers and the CODESYS runtime, which is used by hundreds of device manufacturers in different industrial sectors, including Festo. More information is available on the disclosure blog.

Q: What devices are affected?

A: The table below shows the affected devices for the original disclosure.

Manufacturer	Model	Device type
Bently Nevada	3700, TDI equipment	Condition monitors
Emerson	DeltaV	Distributed control system
Emerson	Ovation	Distributed control system
Emerson	OpenBSI	Engineering workstation
Emerson	ControlWave, BB 33xx, ROC	Remote terminal unit

Emerson	Fanuc, PACsystems	Programmable logic controller
Honeywell	Trend IQ*	Building controller
Honeywell	Safety Manager FSC	Safety instrumented system
Honeywell	Experion LX	Distributed control system
Honeywell	ControlEdge	Remote terminal unit
Honeywell	Saia Burgess PCD	Programmable logic controller
JTEKT	Toyopuc	Programmable logic controller
Motorola	MOSCAD, ACE IP gateway	Remote terminal unit
Motorola	MDLC	Protocol
Motorola	ACE1000	Remote terminal unit
Motorola	MOSCAD Toolbox STS	Engineering workstation
Omron	SYSMAC Cx series, Nx series	Programmable logic controller
Phoenix Contact	ProConOS	Logic runtime
Siemens	WinCC OA	Supervisory Control and Data Acquisition (SCADA)
Yokogawa	STARDOM	Programmable logic controller

The devices affected by the vulnerabilities disclosed on November 29 include controllers running CODESYS V3, Festo CPX-CEC-C1, Festo CPX-MMX and other Festo controllers supporting the FGMC protocol. The full list of affected devices will be provided by the respective manufacturers.

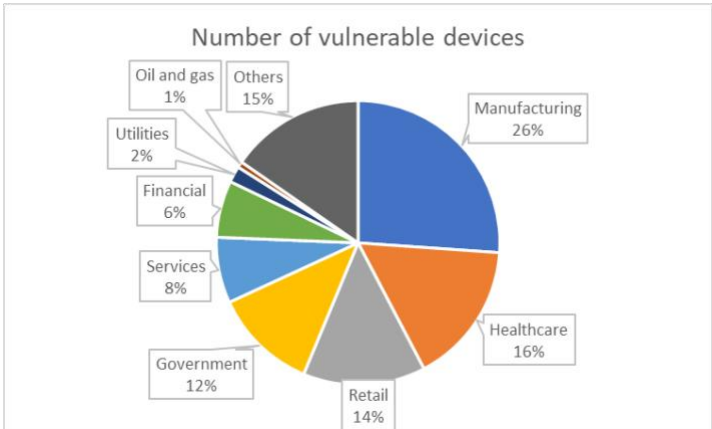
Q: What is the impact of the vulnerabilities?

A: Although the impact of each vulnerability is highly dependent on the functionality each device offers, vulnerabilities fall under the following categories:

- **Remote code execution (RCE)**: Allows an attacker to execute arbitrary code on the impacted device, but the code may be executed in different specialized processors and different contexts within a processor, so an RCE does not always mean full control of a device. This is usually achieved via insecure firmware/logic update functions that allow the attacker to supply arbitrary code.
- **Denial of service (DoS)**: Allows an attacker to either take a device completely offline or to prevent access to some function.
- **File/firmware/configuration manipulation**: Allows an attacker to change important aspects of a device, such as files stored within it, the firmware running on it or its specific configurations. This is usually achieved via critical functions lacking the proper authentication/authorization or integrity checking that would prevent attackers from tampering with the device.
- **Compromise of credentials**: Allows an attacker to obtain credentials to device functions, usually either because they are stored or transmitted insecurely.
- **Authentication bypass**: Allows an attacker to bypass existing authentication functions and invoke desired functionality on the target device.

Abusing these types of insecure by design, native capabilities of OT equipment is the preferred modus operandi of real-world industrial control system (ICS) attackers (e.g., Industroyer2 and INCONTROLLER).

We were able to see more than 5,000 of the affected devices exposed online via Shodan. Most of these are Saia Burgess and OMRON controllers or devices running the ProConOS runtime. We also queried Device Cloud for the vulnerable devices and found close to 30,000 results. The figure below shows the sectors in which the affected devices are most popular. Manufacturing is at the top, with almost one-third of observed devices. After that, we see healthcare, retail and government primarily because of the presence of building automation controllers, since these are industries with many large facilities. We see only a small presence in the OT-intensive oil and gas and utilities sectors, but that is likely because many of those types of customers do not share device information with Forescout's Device Cloud.



Q: Where can I find the full OT:ICEFALL report?

A: The report is available here: https://forescout.com/resources/ot-icefall-report/

Q: How are affected vendors being notified?

A: All affected vendors have been contacted by Forescout and CISA before the disclosure and have had the time to prepare their response.

For the second disclosure in November, Festo and CODESYS were contacted directly by Forescout and included CERT@VDE in the disclosure process.

Q: What can organizations do to mitigate the risk from these vulnerabilities?

A: Complete protection against OT:ICEFALL requires that vendors address these fundamental issues with changes in device firmware and supported protocols and that asset owners apply the changes (patches) in their own networks.

Realistically, that process will take a very long time. In addition to network monitoring, mitigations for OT:ICEFALL include isolating OT/ICS networks from corporate networks and the internet, limiting network connections to only specifically allowed engineering workstations and focusing on consequence reduction where possible. Below, we briefly discuss the most important mitigation strategies for asset owners:

- **Discover and inventory vulnerable devices**. Network visibility solutions enable discovery of vulnerable devices in the network and apply proper control and mitigation actions.

- **Enforce segmentation controls and proper network hygiene** to mitigate the risk from vulnerable devices. Restrict external communication paths and isolate or contain vulnerable devices in zones as a mitigating control if they cannot be patched or until they can be patched.
- **Monitor progressive patches released by affected device vendors** and devise a remediation plan for your vulnerable asset inventory, balancing business risk and business continuity requirements.
- **Monitor all network traffic for malicious packets** that try to exploit insecure-by-design functionality. You should block anomalous traffic or at least alert its presence to network operators.

Further general recommended mitigation is available on CISA's Shields Up initiative that includes the publication Securing Industrial Control Systems and list of recommended practices. Specific mitigation for each vulnerable device will be provided by the respective vendors.

Q: What are the implementation requirements for mitigation using Forescout?

A: Implementing mitigation for OT:ICEFALL requires:

- Extensive visibility on devices and communications based on deep packet inspection
- Segmentation of OT assets
- Continuous network monitoring
- ICS-specific threat and vulnerability hunting capabilities

The Forescout Continuum Platform helps you achieve all these steps without disrupting critical business processes or requiring operational downtime. Forescout's eyeInspect product has native monitoring capabilities for the protocols used by the affected devices and built-in detection for exploitation of OT:ICEFALL vulnerabilities; new vulnerabilities and detections are continuously added to the database and released to customers monthly.

Q: What should I do if I want to learn more about the vulnerabilities?

A: Vedere Labs researchers are available to speak with asset owners that are affected by these vulnerabilities, other researchers and members of the cybersecurity community. To set up a call, please email vederelabs@forescout.com.

Q: Where do I go for more information?

A: For more information on the vulnerabilities and mitigation strategies, reference our original blog and the blog detailing the second disclosure.